

# Minimisasi waktu akses Tor Project menggunakan algoritma greedy

Muhammad Rafid Amrullah - 13515125

Program Studi Teknik Informatika

Institut Teknologi Bandung

Bandung, Indonesia

rafid@s.itb.ac.id

**Abstract**—Dalam mengakses suatu server, baik itu web server, ftp server, dhcp server, proxy server, atau server-server lainnya kita terkadang membutuhkan akses secara anonim menggunakan Tor Project terlepas dari keperluannya baik itu untuk keperluan rahasia, *penetration test*, *surfing anonymously*, hingga aktifitas meretas. Pada umumnya penggunaan Tor Project mengakibatkan kecepatan download dan kecepatan upload data berkurang yang dikarenakan node-node relay yang di lewati pengguna Tor Project saat download atau upload. Oleh karena itu dibutuhkan tools untuk minimisasi waktu akses yaitu menggunakan algoritma greedy pada konfigurasi relay Tor Project yang akan dijelaskan pada makalah ini.

**Keywords**—*greedy*; *tor project*; *anonymous*; *access time*

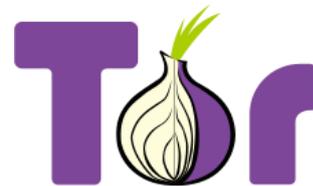
## I. LATAR BELAKANG

Pada umumnya pengguna internet berseluncur secara naif di internet. Hal tersebut memungkinkan identitas network yang digunakan oleh pengguna tersebut dapat diketahui oleh publik. Identitas yang umumnya dapat diketahui publik adalah ip address, network location, computer account, operating system, internet provider, dll.

Banyak hal yang bisa terjadi bila hal tersebut diketahui publik. Pada umumnya identitas pengguna internet digunakan untuk analisis trafik. Contohnya suatu e-commerce bisa saja melakukan diskriminasi harga barang sesuai lokasi negara pengguna yang diketahui dari analisis trafik. Bahkan, keterbukaan terhadap publik ini bisa saja mengancam karir pekerjaan seseorang karena ada informasi pribadi yang mudah dicari orang lain. Dengan kata lain, publik bisa saja mengetahui asal negara dan status karir seseorang, bahkan jika koneksi yang digunakan sudah terenkripsi.

Trafik analisis tersebut mengidentifikasi paket data internet yang diberikan oleh pengirim ke penerima. Paket data internet tersebut memiliki dua bagian: konten dan header. Umumnya trafik analisis akan mengidentifikasi header pada suatu paket data internet yang berada pada suatu network. Dapat diibaratkan trafik analisis berdiam di antara pengirim dan penerima paket data internet kemudian trafik analisis melihat pada setiap header paket data internet yang lewat, bahkan pada jaringan yang terenkripsi, mengingat jaringan yang terenkripsi hanya menyembunyikan konten dari suatu paket data internet yang berada pada lalu lintas data, sedangkan headernya tidak.

Terbukaan terhadap publik tersebut dapat diatasi dengan menggunakan Tor Project. Tor Project atau Tor adalah sebuah software dan jaringan terbuka yang membantu semua orang untuk menghindari analisis trafik, gangguan keamanan jaringan, dan gangguan keamanan negara<sup>[1]</sup>. Tor juga biasa digunakan untuk keperluan rahasia, *penetration test*, *surfing anonymously*, hingga aktifitas meretas. Tor sendiri dioperasikan oleh sebuah grup *volunteer-operated* server yang berbasis di Amerika Serikat.



Gambar 1.1 Tor Project

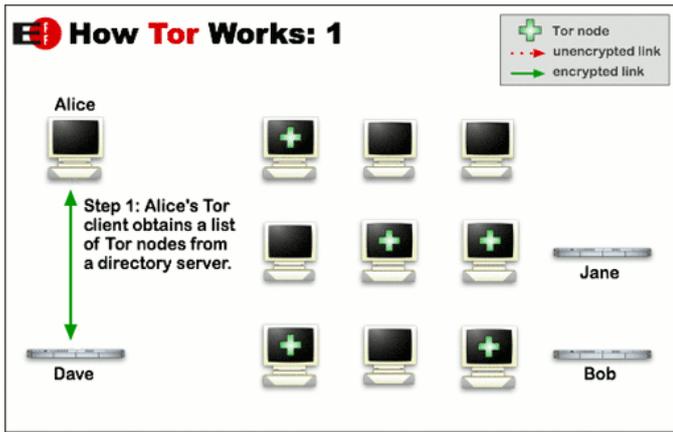
[www.torproject.org](http://www.torproject.org)

Diakses 17 Mei 2017

Tor bekerja dengan mengenkripsi berulang kali tunnel akses yang dilakukan pengguna Tor (disini kita sebut Tor client) terhadap server yang hendak dia akses. Idanya seperti menghilangkan jejak sehingga hal yang membuntuti seperti analisis trafik tidak akan bisa menemukan trafik yang kita lakukan. Cara yang dilakukan Tor untuk menghilangkan jejak adalah dengan menggunakan relay Tor yang tersebar di dunia. Pertama Tor client mengambil daftar seluruh node Tor yang tersedia, kemudian Tor client akan membangun sirkuit yang secara inkremental terenkripsi hingga ujung node Tor yang terdapat pada sirkuit.

Setelah sirkuit terbentuk, banyak data yang dapat dilalui di sana, begitu juga dengan pengembangan software dapat dilakukan. Sirkuit Tor tersebut dapat disebut juga sebagai Tor relay, dimana hampir seluruh sirkuit yang dibentuk merupakan jaringan yang terenkripsi berulang kali secara inkremental. Secara keseluruhan network yang digunakan Tor client merupakan Tor network.

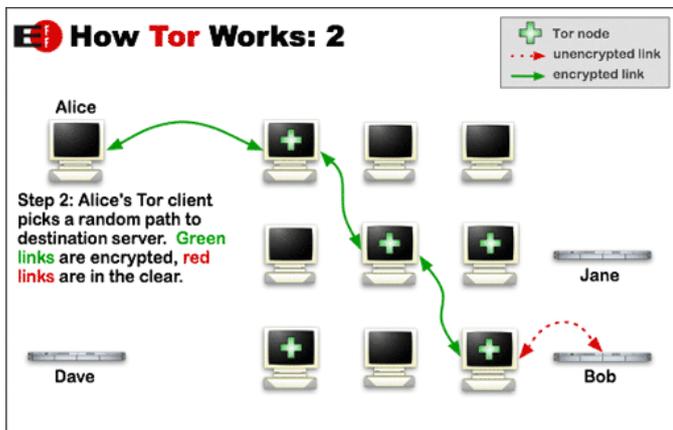
Berikut ilustrasi dari penjelasan di atas :



Gambar 1.2 Pengambilan daftar seluruh node oleh Tor Client

[www.torproject.org](http://www.torproject.org)

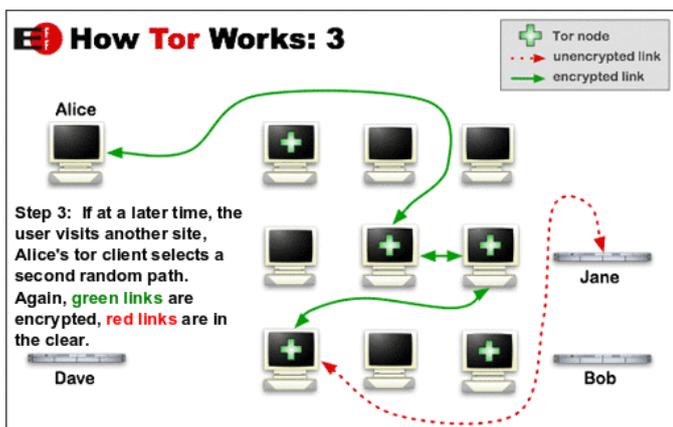
Diakses 17 Mei 2017



Gambar 1.3 Membangun sirkuit Tor dan mengakses node Tor.

[www.torproject.org](http://www.torproject.org)

Diakses 17 Mei 2017



Gambar 1.4 Akses pada node di sirkuit Tor

[www.torproject.org](http://www.torproject.org)

Diakses 17 Mei 2017

Meski Tor adalah tools yang sudah canggih untuk persoalan kemanan, namun Tor memiliki kekurangan dalam waktu aksesnya. Hal tersebut dikarenakan Tor network memiliki banyak node yang perlu Tor user kunjungi.

## II. TUJUAN

Paper ini diharapkan dapat memberi penjelasan dan gambaran mengenai penggunaan algoritma greedy pada penentuan sirkuit Tor (Tor relay). Penggunaan algoritma greedy pada makalah ini mencakup bagaimana mendapatkan sirkuit Tor dengan waktu akses yang paling minimum berdasarkan kalkulasi waktu akses dari satu node ke node lainnya.

## III. DASAR TEORI

Algoritma Greedy merupakan algoritma yang sangat sederhana. Algoritma greedy hanya menentukan pilihan terbaik dari suatu kondisi dan tidak melihat bagaimana hasil akhir yang akan didapat di akhir persoalan secara keseluruhan. Oleh karena itu banyak persoalan yang tidak dapat diselesaikan menggunakan algoritma ini.

Algoritma Greedy memiliki lima parameter:<sup>[3]</sup>

1. Himpunan Kandidat (C)
2. Himpunan Solusi (S)
3. Fungsi Kelayakan (FK)
4. Fungsi Seleksi (FS)
5. Fungsi Objektif (FO)

Algoritma Greedy dapat direpresentasikan sebagai berikut

- Himpunan solusi kosong
- Di setiap langkah:
  - Kandidat solusi (C), akan dicari menggunakan Fungsi Seleksi (FS)
  - Jika solusi layak (FK) maka solusi akan dimasukan ke himpunan Solusi (S)
  - Jika solusi-solusi sudah mencapai fungsi objek tif (FO) maka algoritma berhenti dan solusi yang didapat merupakan jawabannya.<sup>[3]</sup>

Algoritma Greedy sering digunakan untuk beberapa permasalahan seperti permasalahan penukaran uang. Pada permasalahan ini, jumlah koin yang dikembalikan ingin diminimasi.

Fungsi	Deskripsi
Himpunan Kandidat	1,5,10,20,50
Fungsi Seleksi	Koin dengan nilai tertinggi dibawah uang yang harus dikembalikan
Fungsi Kelayakan	Memeriksa apakah solusi melebihi jumlah uang yang diminta
Fungsi Objektif	Jumla koin yang digunakan minimum

Tabel 3.1 Tabel fungsi-fungsi Algoritma Greedy pada persoalan penukaran uang.

Kembalian yang harus didapat adalah 69.

<b>Kondisi Awal</b>	$S = \{ \}$
<b>Langkah 1</b>	$C = \{1,5,10,20,50\}$ $X = FS(C)$ $X = \{50\}$ Apakah $\{50\}$ layak ? Ya, $S = \{50\}$ Apakah $S$ solusi ? Bukan
<b>Langkah 2</b>	$C = \{1,5,10,20,50\}$ $X = FS(C)$ $X = \{10\}$ Apakah $\{50,10\}$ layak ? Ya, $S = \{50,10\}$ Apakah $S$ solusi ? Bukan
<b>Langkah 3</b>	$C = \{1,5,10,20,50\}$ $X = FS(C)$ $X = \{5\}$ Apakah $\{50,10,5\}$ layak ? Ya, $S = \{50,10,5\}$ Apakah $S$ solusi ? Bukan
...	...
<b>Langkah 7</b>	$C = \{1,5,10,20,50\}$ $X = FS(C)$ $X = \{1\}$ Apakah $\{50,10,5,1,1,1\}$ layak ?

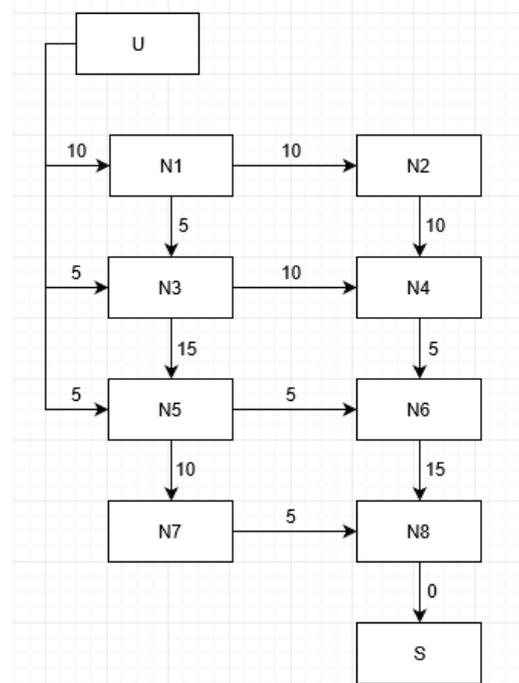
Ya, $S = \{50,10,5,1,1,1\}$ Apakah $S$ solusi ? Iya
--

Program selesai dan solusi yang didapat adalah **{50,10,5,1,1,1}**

#### IV. PERSOALAN

##### A. Deskripsi persoalan

Jika terdapat himpunan kandidat berupa sirkuit Tor yang direpresentasikan seperti ilustrasi berikut:



Gambar 4.1 Ilustrasi Sirkuit Tor

Yang harus kita lakukan adalah mencari jalur dengan total waktu akses paling cepat untuk mencapai  $S$  dari  $U$  dengan syarat harus melewati lebih dari 2 nodes  $N$  Tor agar tunnel koneksi Tor client terenkripsi beberapa kali.

Bila setiap persegi adalah nodes dan panah adalah sirkuit yang tersedia dengan angka yang merepresentasikan waktu akses dari suatu node ke nodes lainnya maka keluaran yang diharapkan adalah waktu akses total yang dibutuhkan untuk mencapai  $S$  dari  $U$  menggunakan algoritma greedy.

Untuk persoalan seperti ini menggunakan algoritma greedy memang kurang efektif, namun terkadang justru membantu dibandingkan dengan menggunakan konfigurasi pengambilan relay Tor secara random yang merupakan konfigurasi default Tor.

### B. Test Case

Case secara tidak langsung akan digenerate otomatis oleh Tor Project karena dalam rentang waktu tertentu terkadang Tor melakukan penutupan dan pembukaan node sehingga penentuan jalur mana yang dilewati secara eksak sangat sulit ditebak, namun yang jelas kita tetap menggunakan algoritma greedy sebagai konfigurasi Tor.

### C. Format Output

Output berupa total waktu yang dibutuhkan untuk mencapai node S dari Tor circuit menggunakan algoritma greedy. Waktu di sini akan didapat dari hasil test menggunakan tester donwload dan upload speed [www.speedtest.net](http://www.speedtest.net). Penggunaan algoritma greedy pada Tor circuit akan diterapkan pada konfigurasi Tor itu sendiri.

## V. DAFTAR SOLUSI

### A. Solusi 1

Solusi ini adalah waktu akses total yang diperlukan untuk mencapai node S dari node U tanpa menggunakan Tor Project, dengan kata lain kita mengakses internet secara biasa tanpa Tor.

### B. Solusi 2

Solusi ini adalah waktu akses total yang diperlukan untuk mencapai node S dari node U menggunakan Tor Project tanpa konfigurasi algoritma greedy, dengan kata lain kita mengakses internet menggunakan Tor yang memiliki konfigurasi default Tor (Pengambilan jalur secara random).

### C. Solusi 3

Solusi ini adalah waktu akses total yang diperlukan untuk mencapai node S dari node U menggunakan Tor Project dan menggunakan konfigurasi algoritma greedy sehingga penentuan jalur mengikuti aturan algoritma greedy.

## VI. IMPLEMENTASI

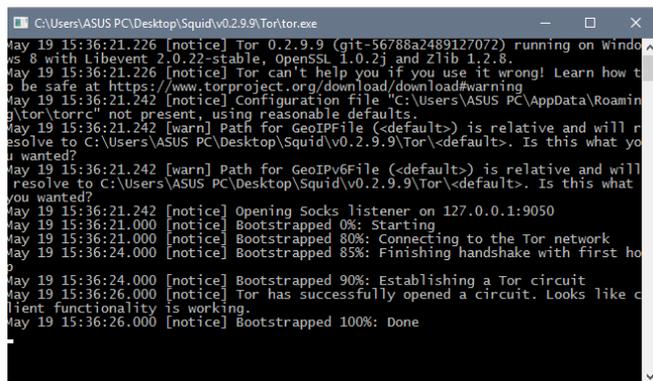
Implementasi algoritma greedy menggunakan parameter-parameternya.

Fungsi	Deskripsi
Himpunan Kandidat	Seluruh node pada circuit Tor
Fungsi Seleksi	Pilih node dengan waktu akses lokal paling kecil
Fungsi Kelayakan	Bila mencapai node S, node N yang tercapai harus lebih dari 2
Fungsi Objektif	Waktu akses paling minimum

**Tabel 6.1** Tabel fungsi-fungsi Algoritma Greedy pada persoalan penukaran uang.

Implementasi menggunakan Tor project yang didownload pada [www.torproject.org](http://www.torproject.org) dan mengubah konfigurasinya sesuai algoritma greedy untuk implementasi solusi 3.

Fungsi Objektif (akses waktu) didapat menggunakan [www.speedtest.net](http://www.speedtest.net) untuk solusi 1, solusi 2, dan solusi 3. Himpunan kandidat adalah seluruh node yang tersedia pada Tor network. Fungsi Seleksi dan Fungsi Kelayakan berada pada konfigurasi Tor Project.



**Gambar 6.1** Penggunaan Tor Project

Eksperimen yang dilakukan menggunakan internet ITB dengan IP 167.205.105.55 dengan target server untuk percobaan adalah server PT. Telkom Indonesia.

## VII. HASIL EKSPERIMEN

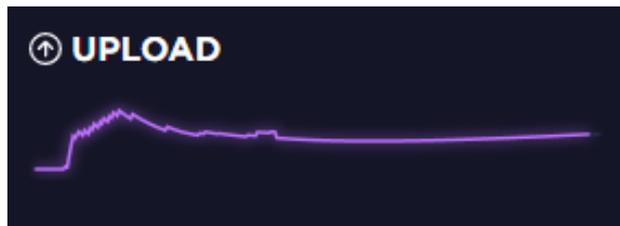
### A. Hasil Eksperimen Solusi 1



**Gambar 6.2** Grafik Download

[www.speedtest.net](http://www.speedtest.net)

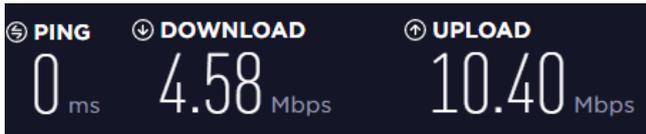
Diakses 18 Mei 2017



Gambar 6.3 Grafik Upload

[www.speedtest.net](http://www.speedtest.net)

Diakses 18 Mei 2017



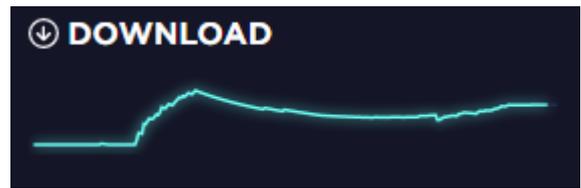
Gambar 6.4 Detail Test

[www.speedtest.net](http://www.speedtest.net)

Diakses 18 Mei 2017

Hasil eksperimen 2 di atas memiliki waktu akses lebih lama dari eksperimen 1 karena eksperimen 2 perlu membuat Tor circuit terlebih dahulu.

### C. Hasil Eksperimen Solusi 3

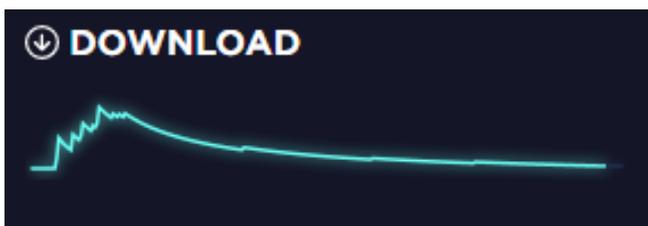


Gambar 6.8 Grafik Download

[www.speedtest.net](http://www.speedtest.net)

Diakses 18 Mei 2017

### B. Hasil Eksperimen Solusi 2



Gambar 6.5 Grafik Download

[www.speedtest.net](http://www.speedtest.net)

Diakses 18 Mei 2017



Gambar 6.9 Grafik Upload

[www.speedtest.net](http://www.speedtest.net)

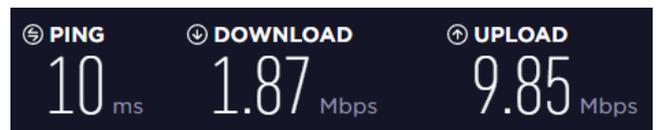
Diakses 18 Mei 2017



Gambar 6.6 Grafik Upload

[www.speedtest.net](http://www.speedtest.net)

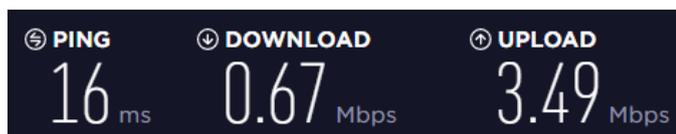
Diakses 18 Mei 2017



Gambar 6.10 Grafik Upload

[www.speedtest.net](http://www.speedtest.net)

Diakses 18 Mei 2017



Gambar 6.7 Detail Test

[www.speedtest.net](http://www.speedtest.net)

Diakses 18 Mei 2017

### VIII. ANALISIS

Kecepatan download/upload berbanding terbalik dengan waktu akses. Maka semakin besar kecepatan download/uploadnya maka waktu akses akan semakin cepat juga. Hal tersebut direpresentasikan pada *ping* yang merupakan kecepatan respon server dalam milisecond.

Dari hasil eksperimen untuk solusi 2 di atas dapat kita bandingkan dengan eksperimen untuk solusi 1 dimana *ping time* untuk eksperimen solusi 1 lebih cepat dibanding dengan eksperimen solusi 2 (menggunakan Tor). Hal tersebut disebabkan oleh circuit Tor yang harus dibentuk terlebih dahulu.

Pada eksperimen untuk solusi 3 (Tor menggunakan konfigurasi algoritma greedy), keadaan membaik. *Ping time* untuk Tor lebih kecil dibandingkan dengan eksperimen untuk solusi 2.

Namun, pada dasarnya eksperimen untuk solusi 3 tidak akan selalu lebih baik dari eksperimen untuk solusi 2 karena pada konfigurasi Tor menggunakan algoritma greedy, optimal yang dicapai dalam waktu akses belum tentu merupakan solusi optimal global, dengan kata lain konfigurasi Tor menggunakan algoritma greedy tidak sepenuhnya akurat.

#### IX. KESIMPULAN

Pada minimisasi akses waktu terkecil untuk Tor Project menggunakan Algoritma Greedy tidak akan selalu menghasilkan solusi terbaik karena pada penentuan waktu akses terbaik hanya dilakukan secara lokal, tidak global.

Namun pada beberapa kasus, Algoritma Greedy untuk konfigurasi Tor Project akan menghasilkan akses waktu yang sangat baik untuk minimisasi waktu akses.

#### ACKNOWLEDGMENT

Saya mengucapkan puji syukur yang sebesar-besarnya kepada Allah SWT atas karuniannya hingga saat ini. Terima kasih kepada Dr. Nur Ulfa Maulidevi, S.T.,M.Sc, Dr.Ir. Rinaldi Munir, M.T, dan Masayu Leylia Khodra, ST., MT atas bimbingannya sehingga penulis dapat mengerti materi perkuliahan Strategi Algoritma. Terima kasih pula kepada

seluruh pihak yang telah membantu penulis dalam mengerjakan makalah ini.

#### REFERENCES

- [1] <https://www.torproject.org/> diakses pada 17 Mei 2017
- [2] Abraham Silberschatz, Greg Gagne, and Peter Baer Galvin, "Operating System Concepts, Eighth Edition ", Chapter 5
- [3] Slide Algoritma Greedy, Rinaldi Munir

#### PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Mei 2017



Muhammad Rafid Amrullah - 13515125